UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/939,531	08/24/2001	Jeffrey Hoffstein	41230/55769	2489

21874 7590 10/13/2004

EDWARDS & ANGELL, LLP
P.O. BOX 55874
BOSTON, MA 02205

EXAMINER	
ZAND, KAMBIZ	
ART UNIT	**PAPER NUMBER**
2132	

DATE MAILED: 10/13/2004

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	09/939,531	HOFFSTEIN ET AL.	
	Examiner	Art Unit	
	Kambiz Zand	2132	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE *3* MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *24 August 2001*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-39* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-5 and 28* is/are rejected.

7)☒ Claim(s) *6-27 and 29-39* is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *24 August 2001* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date *5 and 12/01*.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

DETAILED ACTION

1. **Claims 1-39** have been examined.

2. Foreign Priority benefit claimed under Title 35, United States Code, § 120 have been acknowledged.

Information Disclosure Statement PTO-1449

3. The Information Disclosure Statement submitted by applicant on 12/12/2001 and 03/01/2002 have been considered. Please see attached PTO-1449.

Claim Rejections - 35 USC § 112

4. The following is a quotation of the second paragraph of 35 U.S.C. 112:

The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter, which the applicant regards as his invention.

5. **Claims 2, 7** are rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention.

6. **Claims 2 and 7** recites the limitation "the group", line 2 in the claim. There is insufficient antecedent basis for this limitation in the claim.

Claim Rejections - 35 USC § 102

7. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (b) the invention was patented or described in a printed publication in this or a foreign country or in public use or on sale in this country, more than one year prior to the date of application for patent in the United States.

8. **Claims 1, 3-5 and 28** are rejected under 35 U.S.C. 102(b) as being anticipated by Hardwick et al (5,517,511 A).

As per claims 1 and 28 Hardwick et al (5,517,511 A) teach a method, a computer readable medium containing instructions for a method for performing a cryptographic operation that comprises transforming digital information (see abstract; fig.5-11 where the transformation of digital information is disclosed), the method comprising: providing digital information (see fig.11 where the digital information after priority scanning is disclosed and where the msb and lsb bits are also disclosed); providing a digital operator having a component selected from a large set of elements; expanding the component into a plurality of factors, each factor having a low Hamming weight; and transforming the digital information using the digital operator (see fig.11, 14, 15 and 16; col.4, lines 38-67; col.5, lines 1-45; col.7, lines 10-col.22, line 54).

As per claims 3, 4 and 5 Hardwick et al (5,517,511 A) teach the method of claim 1, wherein the Hamming weight is less than about 30, 20 and 15 (see fig.11, 15 and 18 where hamming weight is disclosed less than 30, 20 or 15).

Claim Rejections - 35 USC § 103

9. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

10. **Claim 2** is rejected under 35 U.S.C. 103(a) as being unpatentable over Hardwick et al (5,517,511 A) in view of Zhao (col.3, lines 35-55).

As per claim 2 Hardwick et al (5,517,511 A) teach all limitation of the claim 1 as disclosed above but do not disclose explicitly the cryptographic operation is selected from the group consisting of key generation, encryption, decryption, creation of a digital signature, verification of a digital signature, creation of a digital certificate, authentication of a digital certificate, identification, pseudorandom number generation and computation of a hash function. However Zhao (col.3, lines 35-55) teach the cryptographic operation is selected from the group consisting of key generation, encryption, decryption, creation of a digital signature, verification of a digital signature, creation of a digital certificate, authentication of a digital certificate, identification, pseudorandom number generation and computation of a hash function (see fig.4-5; col.4, lines 1-38; col.5, lines 46-col.19, line 48 where selection from the above group for crypto operation is repeatedly

disclosed throughout). It would have been obvious to one of ordinary skilled in the art at the time the invention was made to utilize in Hardwick et al's hamming encoding method in order to improve technique for distributing digital presentation by using encryption, authentication, watermarking, certification and digital signature to protect owner's right of their digital presentation as being disclosed by Zhao (col.3, lines 35-55).

Allowable Subject Matter

11. Claims 6, 8-27 and 29-39 are objected to as being dependent upon a rejected base claim, but would be allowable if rewritten in independent form including all of the limitations of the base claim and any intervening claims.

12. Claim 7 would be allowable if rewritten to overcome the rejection(s) under 35 U.S.C. 112, 2nd paragraph, set forth in this Office action and to include all of the limitations of the base claim and any intervening claims.

Conclusion

13. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure:

a. U.S.Patent No. US (5,889,868 A) teach optimization methods for the insertion, protection, and detection of digital watermarks in digitized data.

b. U.S.Patent No. US (5,987,129 A) teach method of sharing cryptokey.

c. U.S.Patent No. US (6,031,911 A) teach practical S box design.

d. U.S.Patent No. US (4,232,194) teach voice encryption system.

e. U.S.Patent No. US (5,764,771 A) teach method for processing a digital signal in a so-called secure communication system and use of this method for access control and/or binary signature.

14. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Kambiz Zand whose telephone number is (703) 306-4169. The examiner can normally reached on Monday-Thursday (8:00-5:00). If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Gilberto Barron can be reached on (703) 305-1830. The fax phone numbers for the organization where this application or proceeding is assigned as (703) 872-9306. Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Kambiz Zand

10/12/04